An improved Spread Spectrum Watermarking technique to withstand Geometric Deformations

A. Sangeetha [1] ,K.Anusudha [2] ,B.Gomathy [3] and K.Surya Tej [4]
[1] asangeetha@vit.ac.in[1]
[2] Kanusudha@vit.ac.in[2]
[3]gomathy_tc16@yahoo.co.in[3]
[4] kunchesuryatej@gmail.com[4]
School of Electrical Sciences
VIT University, Vellore-14

***Abstract*—Here, we propose a new method for the watermarking to withstand the geometric attacks, which may occur during the transmission of the watermarked image. The underlying system is based on Direct Sequence Code Division Multiple Access (DS-CDMA). The algorithm for the normalization has been formulated for use in black and white images. The watermark is spread across the carrier image by using the pseudo-random noise sequences of optimal period and retrieval is made by the use of correlation. Private Key technique is used so the transmission is very secure. Matlab was used to implement the algorithm discussed here.**

I. Introduction

Geometric deformations include rotation, scaling, translation, shearing, random bending, and change of aspect ratio (e.g., [1]–[3]). It is well known that a small amount of rotation and/or scaling can dramatically disable the receiver from detecting the watermark [4].A watermark is robust if it cannot be impaired without also rendering the attacked data useless. Watermark impairment can be measured by criteria such as miss probability, probability of bit error, or channel capacity. Hence, robustness can be evaluated by simultaneously considering watermark impairment and the distortion of the attacked data. The key idea of this watermarking scheme is to use a normalized image for both watermark embedding and detection.

II. Watermarking using CDMA Techniques

The CDMA technique is a spread spectrum technique that spreads the transmitted signal over a wide frequency band, which is much wider than the actual minimum bandwidth required. This technique ensures the survival of watermark under various attacks due to redundancy.

III. Direct Sequence Spread Spectrum

In this form of modulation, a pseudo-random noise generator creates a high-speed pseudo-noise code sequence (sequence of 1 and −1 values). Direct-sequence spread-spectrum transmissions multiply the data being transmitted by this "noise" signal; thus, it directly sets the transmitted radio frequency (RF) bandwidth. The result of modulating an RF carrier with such a code sequence is to produce a direct-sequence-modulated spread spectrum with frequency spectrum, centered at the carrier frequency. The information is demodulated at the receiving end by multiplying the signal by a locally generated version of the pseudo-random code sequence. This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the PN sequence that the receiver believes the transmitter is using.

IV. Watermarking Methodology

The original image is taken and converted into gray scale if required. Normalization procedure is applied to the original image. A PN sequence is generated using a key element, which is confidential to the organization alone. Create a two-dimensional (2-D) watermark with the same size as the normalized image. Binary pseudo-random sequences pi, i=1,2,3…. M is generated, as signature patterns using the private key as seed, where M is the number of bits in the watermark message. Then the last two digits of the sequence will be XORed and the value will be shifted once this process will continue till code of length equal to the length of the cover image is generated. A 1-D DS-CDMA watermark signature by modulating the watermark message with the patterns generated in previous steps is created.

Message is embedded to the normalized image. Desired watermarking strength is used before addition.A mask image is created, which is a binary image of the same size as the normalized image. This image has 1s within the support of the normalized image and 0s elsewhere. Using the mask image the boundary is masked of if it is excess than the cover image.Inverse normalization is done to this watermark embedded image. This is the watermarked image and this is transmitted.

In the receiver side the image is normalized. Using the same key PN sequence is again generated. Correlation is performed between the watermarked image and the PN sequence. Mean of the correlation values are taken and a threshold is fixed. Message is decoded using this threshold.

DOI: 01.ijsip.01.01.07

V. IMPLEMENTATION

The parameters by which the image is normalized are estimated from the geometric moments of the image [4].

A. Image Moments and Affine Transforms

Let f (x, y) denote a digital image of size M x N. Its geometric *moments* m_{pq} and μ_{pq} *central moments*, p, q = 0, 1, 2, 3… are defined, respectively as

$$m_{pq} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} x^p y^q f(x,y)$$

And

$$\mu_{pq} = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} (x-\bar{x})^p (y-\bar{y})^q f(x,y)$$

Where

$$\bar{x} = \frac{m_{10}}{m_{00}}, \bar{y} = \frac{m_{01}}{m_{00}}$$

An image g (x,y) is said to be an *affine transform* of f(x,y) if there is a matrix $A = \begin{pmatrix} a_{11} & a_{21} \\ a_{12} & a_{22} \end{pmatrix}$

and the vector $d = \begin{pmatrix} d_1 \\ d_2 \end{pmatrix}$ such that f(x,y)=g(x,y),

where

$$\begin{pmatrix} x_a \\ y_a \end{pmatrix} = \mathbf{A} \cdot \begin{pmatrix} x \\ y \end{pmatrix} - \mathbf{d}.$$

B.Normalization procedure

The four steps of normalization are:

❖Center the image f (x,y); this is achieved by setting the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and the

Vector with $d = \begin{pmatrix} d1 \\ d2 \end{pmatrix}$ with,

$$d_1 = \frac{m_{10}}{m_{00}}, \quad d_2 = \frac{m_{01}}{m_{00}}$$

Let $f_1(x, y)$ denotes the resulting centered image.

❖Apply a shearing transform to $f_1(x, y)$ in the x direction with matrix $A_x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$

So that the resulting image denoted by, f 2(x,y) = Ax[f1(x,y)].β can be calculated using the formula,

$$\mu_{30}^{(2)} = \mu_{30}^{(1)} + 3\beta\mu_{21}^{(1)} + 3\beta^2\mu_{12}^{(1)} + \beta^3\mu_{03}^{(1)}$$

In particular, we may have the following two scenarios:

1) One of the three roots is real and the other two are complex, we select the real root
2) All three roots are real, then we pick the median of the three real roots.

❖Apply a shearing transform to $f_2(x, y)$ in the y direction with matrix $A_y = \begin{pmatrix} 1 & 0 \\ \gamma & 1 \end{pmatrix}$

So that the resulting image, denoted by, $f_3(x, y) = A_y [f_2(x, y)]$. γ Can be calculated using the formula,

$$\mu_{11}^{(3)} = \gamma\mu_{20}^{(2)} + \mu_{11}^{(2)}.$$

By putting $\mu_{11}^{(3)} = 0$ we get

$$\gamma = -\frac{\mu_{11}^{(2)}}{\mu_{20}^{(2)}}.$$

❖ Scale f 4(x, y) in both x and y directions with $A_s = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ so that the resulting image denoted by,

$f_4(x,y) = As[f_3(x,y)]$ achieves

1) A prescribed standard size.
2) $\mu_{50}^{(4)}>0$ and $\mu_{05}^{(4)}>0$.

Where, α= Standard image size/number of columns in y-sheared image.

β=Standard image size/number of rows in y-sheared image.

The final image $f_4(x, y)$ is the normalized image**.**

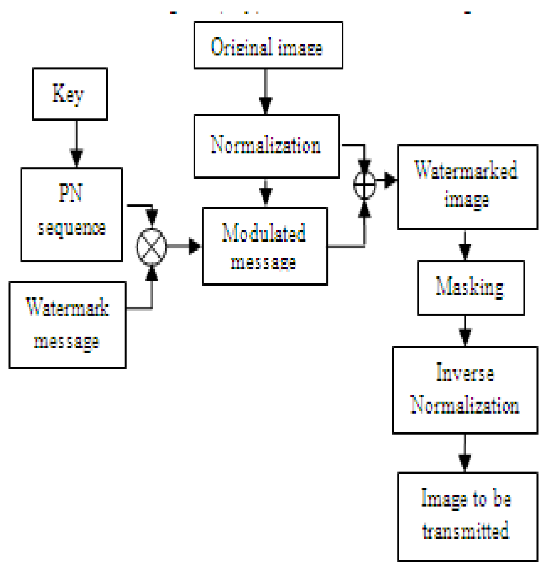


Figure 1. Block diagram

C.Embedding

The addition of the PN sequences to the cover image is done according to the equation:

$$Iw (x, y) = I (x, y) + k \times W (x, y)$$

This is shown in figure given bellow

Where, *Iw (x, y)* denotes the watermarked image.

I (x, y) denote the actual cover image.

W (x, y) denotes a pseudorandom noise pattern that is added to the image.

K denotes the gain factor.

DOI: 01.ijsip.01.01.07

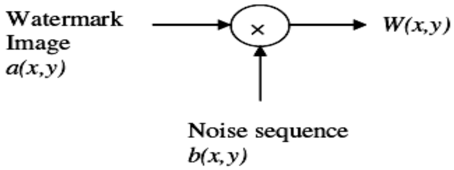


Figure 2(a) Embedding process step-1

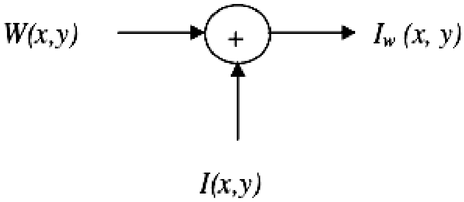


Figure 2(b) Embedding process step-2

D.Extraction

The multiplier output *C* of figure.3 is given by

$$C = Iw(x, y) \times b(x, y)$$
$$= (a(x,y) \times b(x,y) + I(x,y)) \times b(x,y)$$
$$= a(x,y) \times b\text{^}2(x,y) + I(x,y) \times b(x,y)$$

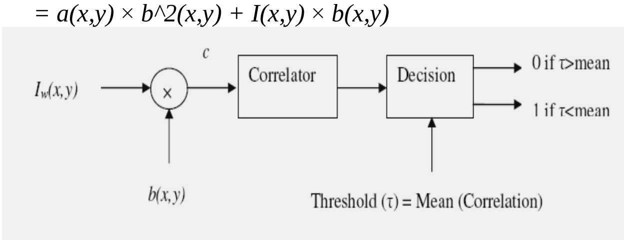


Figure.3 extraction process

The watermark image *a (x, y)* is multiplied twice with the noise signal *b (x, y)* which becomes 1 whereas the unwanted or the cover image *I (x, y)* is multiplied only once with the noise signal that can be filtered out during the process of correlation by setting the threshold as mean of correlation.

$$\text{Correlator Decision} = \begin{cases} 0 \text{ if } \tau > \text{mean} \\ 1 \text{ if } \tau < \text{mean} \end{cases}$$

VI. RESULT ANALYSIS

The first step is normalization.

Figure 4(a) original image

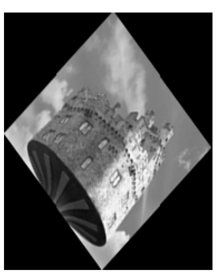


Figure 4(b) normalized image

Then the watermark is embedded.

Figure 5(a) watermark message

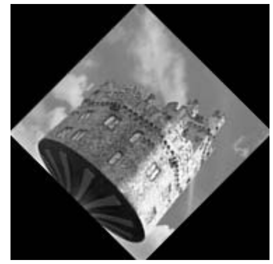


Figure 5(b) watermarked image

This image is masked to remove borders in watermark message if greater than normalized image. To the normalized and masked image inverse normalization is done. Inverse normalization involves the steps, which is simply the inverse of the steps involved in normalization.

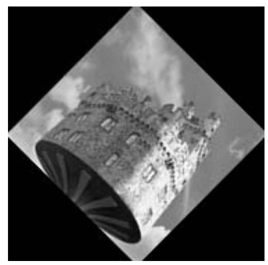


Figure 6(a) masked image

Figure 6(b) image to be transmitted

Receiver side results for a watermarking strength K= 2

Figure 7(a) received image

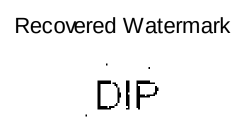


Figure 7((b)recoverd watermark

This difference image below shows that the technique ensures high degree of fidelity. As the gain is increased from 2 to 4, the recovery of the watermark improves, but at the cost of distorting the watermarked image.

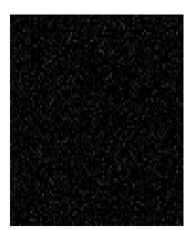
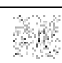


Figure 8. Difference image

DOI: 01.ijsip.01.01.07

VII. Attacks

TABLE I. Comparison between Watermark Recovery with and without Normalization

Type of attack	With normalization	Without Normalization
Line & column Removal		
Scaling		
Aspect ratio Change		
Shearing		
Affine Transformation		
Horizontal Flipping		
Vertical Flipping		
Median filtering		

The above shows the watermarking recovery with and without normalization. From the recovered images it is seen that the normalization procedure resulted in a better geometric deformation resistance to the images.

VIII. Bit Error Ratio

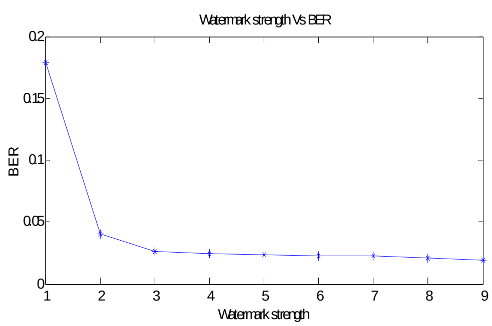


Figure 9. Plot between watermark strength Vs BER

From the plot we can infer that the Bit Error rate decreases with the increase in watermark strength.

A .BER after Geometric Distortion

* Flipping

TABLE II. BER for flipping

Flipping	BER
Horizontal / Vertical	0.0443

* Scaling

TABLE III. BER for scaling

Scaling	BER
0.75	0.0461
0.5	0.0461
1.1	0.0461
1.5	0.0425

* Aspect ratio change

TABLE IV. BER for change of aspect ratio.

Aspect Ratio	BER
(1, 0.8)	0.0490
(1, 0.9)	0.0437
(1, 1.1)	0.0437
(1, 1.2)	0.0514

* Line and column removal

TABLE V. BER for line & column removal

Number of Rows & Columns	BER
(1, 1)	0.0425
(17, 5)	0.0443

* Shearing

TABLE VI. BER for shearing

Shearing	BER
(0, 1%)	0.0319
(5%, 5%)	0.0461

* General geometric affine transformation

TABLE VII. BER for general geometric affine transformation

Matrix	BER
$\begin{pmatrix} 1.1 & 0.2 & 0 \\ -0.1 & 0.9 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	0.1329
$\begin{pmatrix} 0.9 & -0.2 & 0 \\ 0.1 & 1.2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	0.1010
$\begin{pmatrix} 1.01 & 0.2 & 0 \\ -0.2 & 0.8 & 0 \\ 0 & 0 & 1 \end{pmatrix}$	0.0691

DOI: 01.ijsip.01.01.07

IX. CONCLUSION

The proposed algorithm achieves its robustness by both embedding and detecting the watermark message in the normalized images. It is demonstrated that the proposed algorithm can achieve very low decoding BER when used with multi bit watermarks under various affine attacks. From the analysis, the gain factor k=2 is arrived which gives a good balance between the visual quality and watermark robustness. The above process provides high security to the copyright information and preventing access from unauthorized users.

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Attacks on copyright marking systems," in *Proc. Workshop Information Hiding*, Portland, OR, Apr. 1998, pp. 15–17.

[2] M. Kutter and F. A. P. Petitcolas, "A fair benchmark for image watermarking systems," presented at the Electronic Imaging, Security and Watermarking of Multimedia Contents, vol. 3657, Sans Jose, CA, Jan. 1999.

[3] J. Cox and J. P. M. G. Linnartz, "Public watermarks and resistance to tampering," presented at the IEEE Int. Conf. Image Processing, vol. 3, 1997.

[4] C. Y. Lin, M.Wu, J. A. Bloom, I. J. Cox, M. Miller, and Y. M. Lui, "Rotation, scale, and translation resilient public watermarking for images," *IEEE Trans. Image Process.*, vol. 10, no. 5, pp. 767–782, May 2001

[5] M. Alghoniemy and A. H. Tewfik, "Geometric distortion correction through image normalization," presented at the ICME Multimedia Expo, 2000.

[6] Ingemar J. Cox, et al., "Secure Spread Spectrum Watermarking for Multimedia", IEEE *Trans. on Image Processing*, Vol. 6, No.12, Dec 1997, pp.1673-1687.

[7] D. Shen, and Horace H., "Generalized Affine Invariant Image Normalization," *IEEE*Trans. *Pattern Anal. and Machine Intelligence,* Vol. 19, No. 5, pp. 431-440, May 1997.

DOI: 01.ijsip.01.01.07